PISCES
Progressive Information, Security, Computer, and Embedded System

E-ISSN: 2986-7258
P-ISSN : 2986-724X

PISCES Volume 02 Nomor 01 Maret 2024

Protokol Keamanan pada Wireless Sensor Network (WSN) Menggunakan Firewall Iptables dan Enkripsi Base64

[1*]Abdul Wahid, [2]Satria Gunawan Zain, [3]Jumadi Mabe Parenreng, [4]Ilham Juliady

[1,2,3,4] Universitas Negeri Makassar, Jl. A.P. Pettarani, Makassar, Sulawesi Selatan

Email: wahid@unm.ac.id[1], satria.gunawan.zain@unm.ac.id[2], jparenreng@unm.ac.id[3,] juliadiilham27@gmail.com

Received : 15 Januari 2024
Accepted : 19 Februari 2024
Published : 10 Maret 2024

ABSTRAK

Pada saat ini era teknologi yang semakin pesat dan modern seperti sistem *Internet of Things* (IoT) yang sebagian besar telah diterapkan pada kehidupan sehari-hari untuk memudahkan setiap aktivitas manusia. Seperti penerapan *Wireless Sensor Network* (WSN). Setiap penerapan layanan jaringan publik memiliki celah. Hal tersebut sangatlah merugikan pada sebuah perusahaan yang menerapkan teknologi sistem *Wireless Sensor Network* (WSN) jika server diretas maka data-data yang sistem akan diketahui oleh peretas. Untuk itu, dibutuhkan suatu metode agar keamanan server dan dan proses transfer data lebih terjamin. Metode yang digunakan dengan melakukan penerapan firewall iptables dan Enkripsi data menggunakan Enkripsi Base64 yang jika metode ini diterapkan maka server dan setiap data yang dikirim dalam komunikasi 2 arah akan dijamin aman dari pembacaan data dan peretasan server. Sehingga metode ini dapat digunakan untuk meningkatkan keamanan Data dan keamanan server.

Kata Kunci: Iptables, Firewall, Enkripsi, Enkripsi Base64, Keamanan Data, Data Server

ABSTRACT

Currently, the era of technology is getting faster and more modern, such as the Internet of Things (IoT) system, most of which have been implemented in everyday life to facilitate every human activity. Such as the application of Wireless Sensor Network (WSN). Every network service implementation has a public loophole. This is very detrimental to companies that implement Wireless Sensor Network (WSN) system technology. If the server is hacked, the data on the system will become known to the hacker. For this reason, we need a way so that server security and data transfer processes are guaranteed. The method used is implementing an iptables firewall and encrypting data using Base64 encryption, where if this method is implemented then the server and any data sent in 2-way communication will be guaranteed safe from data reading and server hacking. So this method can be used to improve data security and server security.

Keywords: *Iptables, Firewall, Encryption, Base64 Encryption, Data Security, Server Data.*

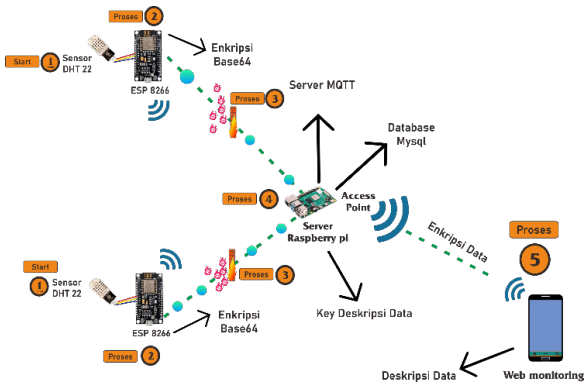
1. PENDAHULUAN

Penerapan teknologi yang meningkat secara signifikan telah mengubah kehidupan manusia menjadi lebih modern dan praktis, seperti penggunaan alat yang semakin praktis dan mudah digunakan oleh user [1]. Penggunaan alat yang digunakan seperti monitoring dan kendali jarak jauh yang tentunya menggunakan wifi publik untuk menghubungkan perangkat server dan perangkat user [2]. Penerapan *Wireless Sensor Network* (WSN) memiliki beberapa titik sensor yang datanya dikumpulkan dalam 1 server dan selanjutnya akan diteruskan pada sistem monitoring [3]. Tentunya pada sebuah teknologi *monitoring* menerapkan sebuah konsep *Internet oF Things* (IoT) yang dikolaborasikan dengan *Wireless Sensor Network* (WSN) [4]. Menguhubungkan perangkat keras seperti *node* sensor dan *Mikrokontroler* yang akan mengirimkan informasi ke *software monitoring* melalui jaringan internet [5]. Namun jaringan internet rentan terhadap keamanan jaringan [6]. Melihat saat ini sangat banyak kasus peretasan server dan kebocoran data yang terjadi maka pada sistem *Wireless Sensor Network* (WSN) ini harus melakukan sebuah pendekatan untuk mengamankan server [7]. Maka sistem harus memiliki peningkatan keamanan jaringan dan transfer data [8]. Menerapkan sebuah teknik enkripsi agar tidak rentan terhadap serangan yang dapat menganggu kinerja server dan percobaan pembacaan serta manipulasi data [9]. Keamanan data yang menggunakan Enkripsi Base64 bisa menjadi solusi [10]. Tujuannya agar tidak ada pihak lain yang bisa membaca data saat proses transfer data pada server [11]. Sehingga dengan menerapkan teknik firewall iptables dan Enkripsi Base64 server maka transfer data akan terjamin aman dari pembacaan dan kebocoran data [12]. karena Ketika Mikrokontroler menangkap data dari Sensor maka terjadi sebuah proses Enkripsi pada mikrokontroler dan berubah menjadi data acak atau data yang tidak dapat dibaca [13]. Ketika data tersebut ditransfer maka akan terjadi filtering *ip address* yang dikenali dapat mengakses server dan *ip address* yang tidak dikenali akan diblokir [14]. Maka dengan menerapkan metode tersebut pada *Wireless Sensor Network* (WSN) maka jaringan dan server akan terjamin aman dari kebocoran data dan peretasan server [15].

2. METODE PENELITIAN

2.1 Arsitektur Global sistem keamanan

Secara arsitektur global sistem ditunjukkan pada gambar berikut. Dimana dapat dilihat kompenen-kompenen yang membentuk dan membangun sebuah sistem *Secure Wireless Sensor Netwrok* pada penelitian ini. Ikon kompenen yang digunakan pada gambar arsitektur global sistem ini merupakan ilustrasi sistem keamanan jaringan dan enkripsi data yang diimplementasikan.

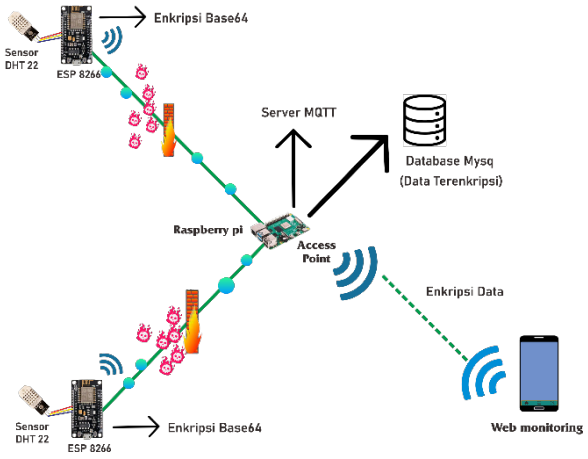


Gambar 1 Ilustrasi global sistem

2.2 *Firewall Iptables*

Secara arsitektur sistem ditunjukkan pada gambar berikut. Dimana dapat dilihat kompenen-kompenen yang membentuk dan membangun sebuah sistem *Secure Wireless Sensor Network* pada penelitian ini. Ikon

kompenen yang digunakan pada gambar arsitektur global sistem ini merupakan ilustrasi sistem keamanan jaringan akan diimplementasikan.

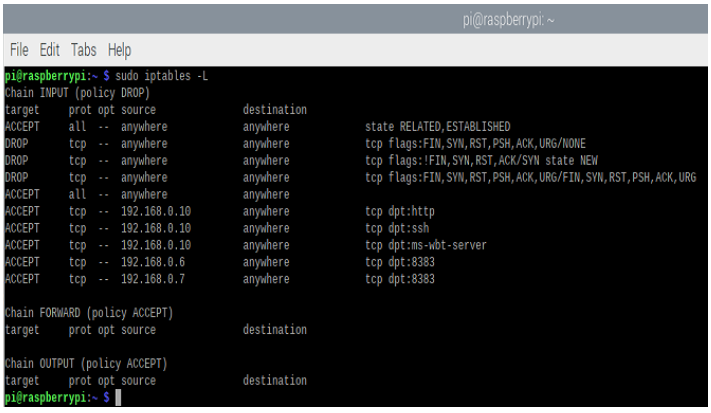


Gambar 2 Ilustrasi firewall iptables

Ilustrasi pada Gambar 2 yaitu Upaya dalam meningkatkan keamanan data agar tidak semua orang dapat mengakses database dan tidak dapat dimanipulasi dari serangan *hacker*. Prinsip kerja dari Sistem *security* menggunakan *firewall Shorewall Iptables* akan memblokir Ip Address yang tidak diketahui, maka hanya Ip address yang diketahui dapat mengakses database.

2.3 Konfigurasi *Firewall Iptables*

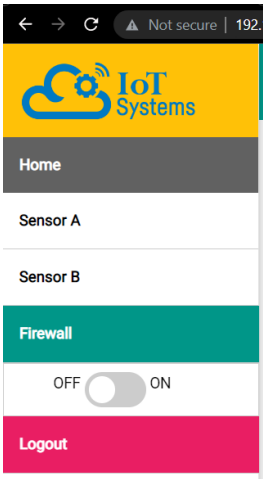
Melakukan sebuah konfigurasi firewall iptables pada *raspberry pi* ini untuk filtering semua akses yang akan masuk ke server *raspberry pi*. konfigurasi atau pembuatan rules *firewall* ini dimana akan membuka port tertentu yang akan diakses oleh *Ip address* tertentu yang akan di izinkan. *Ip address* yang di izinkan adalah Ip dari Esp 8266 yaitu *192.168.0.6* dan *192.168.0.7* maka hanya dengan ip tersebut lah yang dapat masuk untuk mengakses server *raspberry pi*.



Gambar 3 Rules Konfigurasi Iptables

2.4 Pembuatan fitur *on/off firewall* pada website

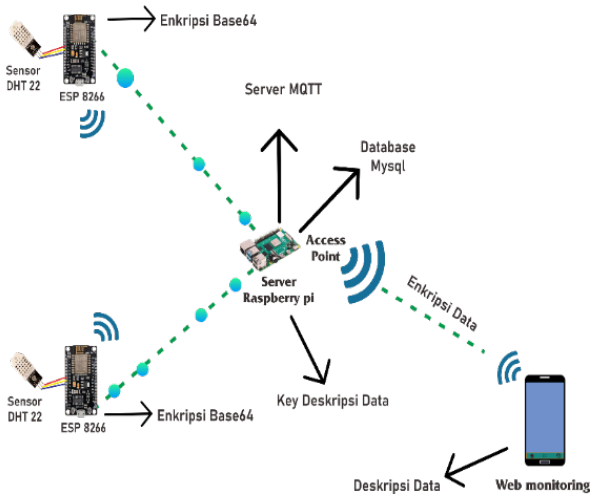
Melakukan pembuatan fitur aktifkan/ nonaktifkan *firewall* pada website dengan menggunakan Bahasa pemrograman *PHP* dan setiap mengaktifkan/ nonaktifkan *firewall* pada website akan terkeram di server *raspberry pi.* Hal ini dilakukan dengan tujuan agar Admin dengan mudah mengaktifkan / nonaktifkan *firewall.*



Gambar 4 Fitur On/Off Firewall pada website

2.5 Arsitektur Enkripsi Base64

Secara arsitektur global sistem ditunjukkan pada gambar berikut. Dimana dapat dilihat kompenen-kompenen yang membentuk dan membangun sebuah sistem *Secure Smart Farming* pada penelitian ini. Ikon kompenen yang digunakan pada gambar arsitektur Enkripsi sistem ini merupakan ilustrasi sistem keamanan data yang nantinya akan diimplementasikan.

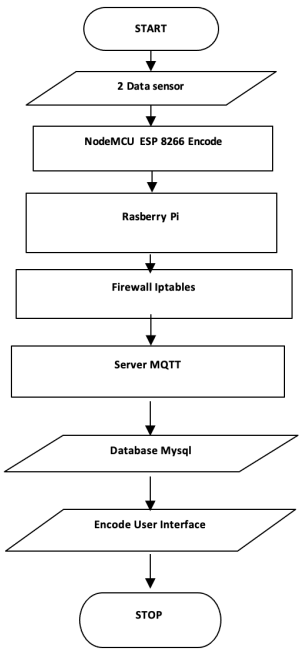


Gambar 5 Arsitektur Enkripsi

Ilustrasi pada Gambar 5 yaitu Upaya dalam meningkatkan keamanan data agar tidak semua orang dapat mengakses database dan tidak dapat dimanipulasi dari serangan *hacker*. Sebelum Prinsip kerja dari Sistem *security* menggunakan *Enkripsi Base64* ini Ketika ESP 8266 menangkap data dari sensor DHT 22 maka terjadi proses enkripsi lalu mengirim ke Server MQTT raspberry pi dan Ketika web monitoring memanggil untuk ditampilkan maka Decode pada raspberry pi server akan bekerja.

Mekanisme kerja dari sistem ini dapat kita lihat pada gambar 6 yaitu sebuah flowhart atau tahapan mekanisme sistem bekerja yaitu ketika semua alat aktif, maka ke dua sensor DHT 22 akan bekerja untuk mendeteksi suhu dan kelembapan setelah itu data akan ter enkripsi pada Esp 8266 lalu Mikrokontroler Esp 8266 akan mengirimkan data pada Raspberry pi dan ketika dalam proses pengiriman data ke raspberry pi akan diamankan dengan Firewall iptables. Firewall Iptables ini akan memblokir akses jaringan yang tidak sah, maka hanya 2 Esp 8266 yang dapat mengakses server. Setelah itu data akan tersimpan pada Server Mqtt dan Database Mysql lalu ketika interface memanggil untuk menampilkan data maka secara otomatis decode akan bekerja untuk mengubah data acak menjadi data asli.

2.6 Flowchart Sistem



Gambar 6 Flowchart sistem

2.7 Program encode data Arduino ESP 8266

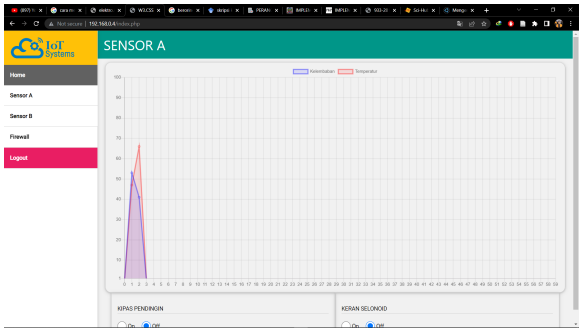
Melakukan codingan pada Arduino IDE menggunakan Bahasa pemrograman C dan memanfaatkan library Arduino IDE yaitu Base64 dengan tujuan untuk mengamankan data sensor yang akan dikirim ke server raspberry pi. Ketika ESP 8266 melakukan transfer data ke server raspberry pi, proses enkripsi dimana data asli dalam bentuk angka dan akan terconvert menjadi data string yang tidak dikenali atau data yang telah dienkripsi dan setelah proses tersebut terjadi maka Mikrontroler ESP 8266 akan melakukan transfer data ke server raspberry pi.

2.8 Konfigurasi decode Base64

Konfigurasi decode Base64 di server raspberry pi menggunakan Bahasa pemrograman python. Decode base64 merupakan sebuah key atau kunci dari enkripsi Base64 yang dikirim dari ESP 8266 maka dengan hal tersebut Ketika data sensor telah diterima pada server raspberry pi lalu akan diteruskan ke database mysql maka key base64 akan bekerja untuk membuka kunci enkripsi menjadi data asli. Ketika proses key enkripsi bekerja dengan cara mengconvert Kembali data string enkripsi menjadi data char atau dalam bentuk angka. Maka dengan hal tersebut data yang akan tampil yaitu data sensor asli yaitu suhu dan kelembapan.

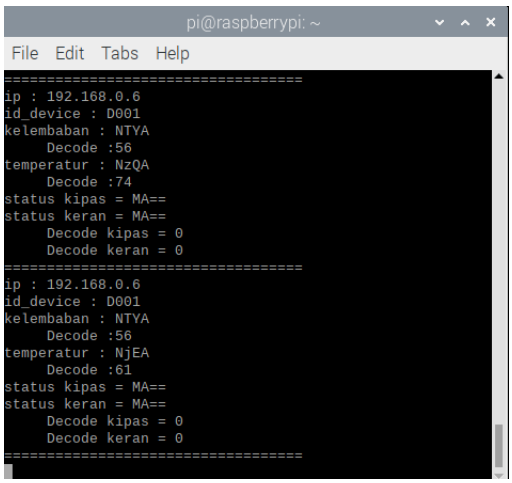
2.9 Hasil Decode Base64

Pada Gambar 7 merupakan website monitoring suhu dan kelembapan pada wireless sensor network (WSN). Data yang ditampilkan merupakan data asli yang awalnya di enkripsi dan Ketika Web monitoring memanggil untuk ditampilkan maka Encode akan bekerja lalu menampilkan data asli. Maka metode enkripsi ini berhasil diterapkan pada Wireless Sensor Network (WSN) dan data dijamin aman dari pembacaan data oleh pihak lain atau pihak yang tidak bertanggung jawab (Hacker).



Gambar 7 Website Monitoring

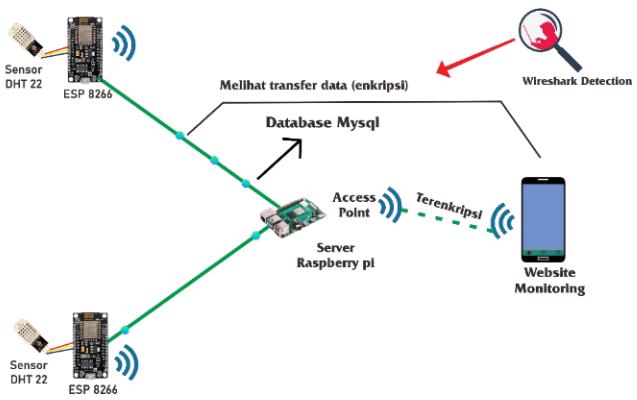
2.10 Server Mqtt Raspberry pi



Gambar 8 Server MQTT raspberry pi

Pada Gambar 8 merupakan Server MQTT raspberry pi yang menampilkan data enkripsi dan data asli. Server tesebut juga berfungsi dalam pengiriman data untuk ditampilkan pada website monitoring. Melakukan sebuah konfigurasi server MQTT pada raspberry pi menggunakan Bahasa pemrograman Python. Konfigurasi server ini dilakukan untuk menyimpan semua data-data yang dikirim dari Mikrokontroler ESP 8266 akan tersimpan di server raspberry pi. Maka dengan demikian *raspberry pi* akan dimanfaatkan menjadi server utama lalu diteruskan kepada database mysql untuk ditampilkan pada website localhost.

2.11 Skenario Uji Coba



Gambar 9 ilustrasi serangan

Skenario uji coba ini dilakukan untuk melihat tingkat keberhasilan setelah menerapakan enkripsi data menggunakan Enkripsi Base64 pada *Smart Farming* Budidaya Jamur Tiram. Simulasi penyerangan dengan menggunakan *tools kali linux wireshark* untuk scanning aliran jaringan dan melihat data yang ditransfer.

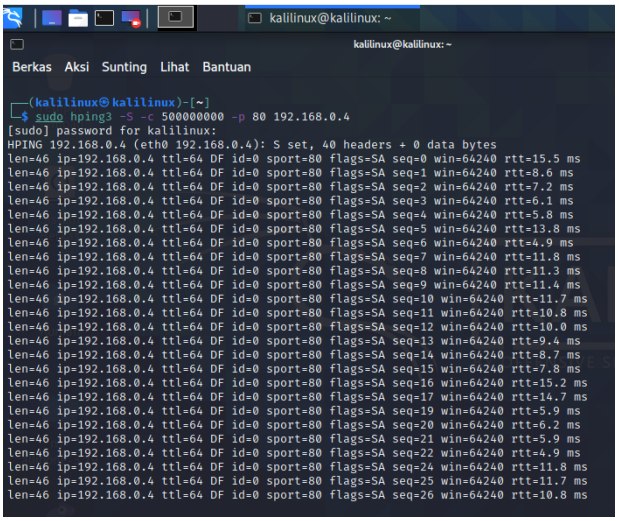
3. HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Hasil penelitian ini berupa peningkatan keamanan pada sistem *Internet of Things* (IoT) dan *Wireless Sensor Network* (WSN) yang di implementasikan pada *Smart Farming* Budidaya jamur tiram berbasis *Wireless Sensor Network* (WSN). Pengembangan pada sisi keamanan *smart farming* ini bertujuan untuk meningkatkan keamanan pada sebuah sistem dan terkhusus sistem *Internet of Things (IoT)* dalam upaya meningkatkan keamanan setiap komunikasi transfer data serta kendalinya. Karena konsep dasar *Internet of Things (IoT)* dengan memanfaat jaringan internet dalam transfer data sehingga sistem dapat aman dari serangan.

3.2 Skenario Pengujian Firewall Iptables

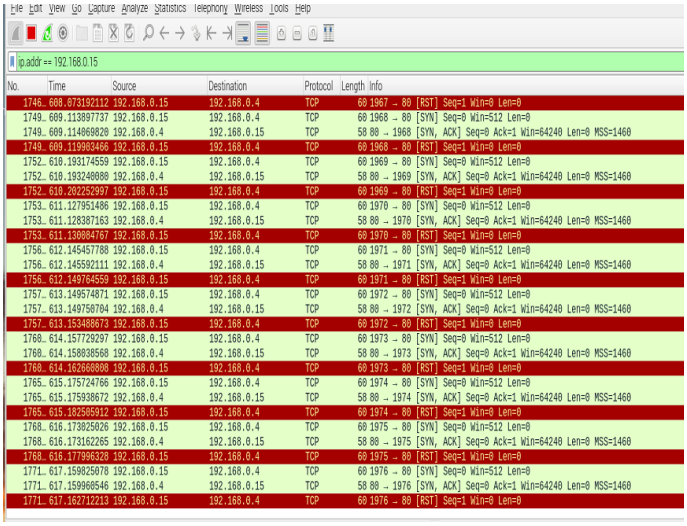
Pengujian *firewall* menggunakan *DDOS Attack* atau *Hping3* dilakukan untuk mencoba untuk membanjiri paket masuk ke server sehingga terjadi penurunan performa pada server, jika server *down* maka pengiriman data tidak dapat melakukan pelayanan dengan baik. Hal tersebut sangatlah merugikan bagi sistem *Wireless Sensor Network* (WSN) yang dikolaborasikan dengan *Internet of Things* (IoT) yang menggunakan jaringan internet dalam berkomunikasi dan saling mengirim data antar client dan server. Maka hal ini perlu solusi agar sistem *Wireless Sensor Network* (WSN) dapat dipercaya beroperasi dengan baik tanpa ada gangguan terhadap pihak yang tidak bertanggung jawab dengan memanfaatkan jaringan internet untuk merusak sistem.



Gambar 10 Serangan Ddos Attack masuk ke server

3.3 *Capture Traffic network DDOS attack* ke server

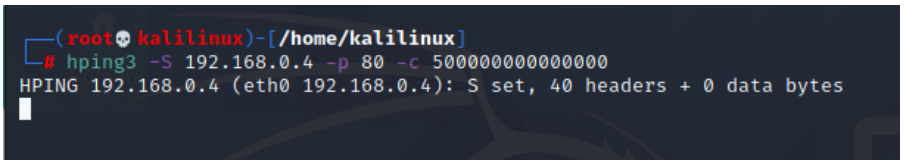
Bisa kita lihat yang berwarna merah tersebut merupakan penyerangan *DDOS Attack* atau pembanjiran paket yang masuk ke server dan terdeteksi dari *Ip Address* 192.168.0.15. *Ip Address* Tersebut merupakan sumber serangan yang terjadi dari Komputer client Asing.



Gambar 11 Kondisi trafik jaringan firewall off

3.4 Pengujian *firewall* ketika aktif

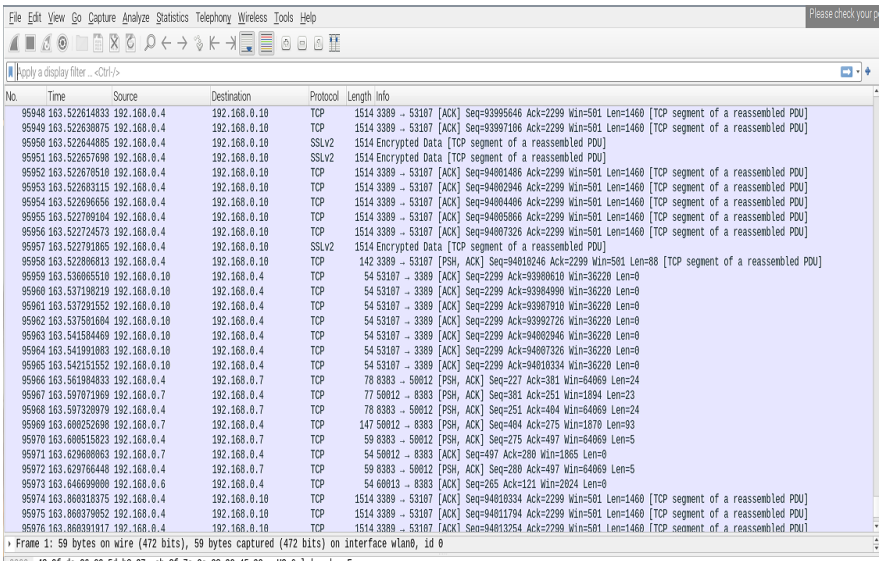
Pengujiann keamanan Ketika *firewall* diaktifkan, Ketika *firewall* diaktifkan maka serangan dari *Ip Address* yang telah diblokir maka tidak bisa melakukan pembanjiran paket menggunakan *DDOS Attack.*



Gambar 12 Kondisi trafik jaringan firewall On

3.5 Kondisi trafik jaringan

Traffic jaringan Ketika *firewall* memblokir *Ip Address* yang melakukan *DDOS* Attack. *Traffic* jaringan menjadi normal dan aman karena *firewall* telah berhasil memblokir *Ip Address* yang melakukan serangan.



Gambar 13 Kondisi trafik jaringan firewall On

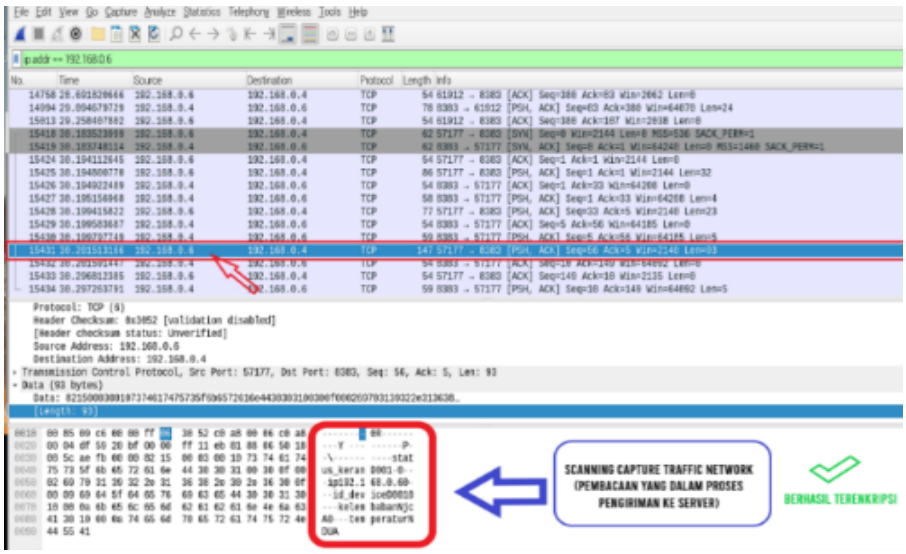
3.6 Hasil Pengujian Firewall Iptables

Table 1 Hasil pengujian firewall

No	Source	Destination	Firewall
1	192.168.0.6	192.168.0.4	Terakses
2	192.168.0.7	192.168.0.4	Terakses
3	192.168.0.15	192.168.0.4	Diblokir
4	192.168.0.16	192.168.0.4	Diblokir
5	192.168.0.17	192.168.0.4	Diblokir
6	192.168.0.18	192.168.0.4	Diblokir
7	192.168.0.19	192.168.0.4	Diblokir
8	192.168.0.20	192.168.0.4	Diblokir
9	192.168.0.21	192.168.0.4	Diblokir

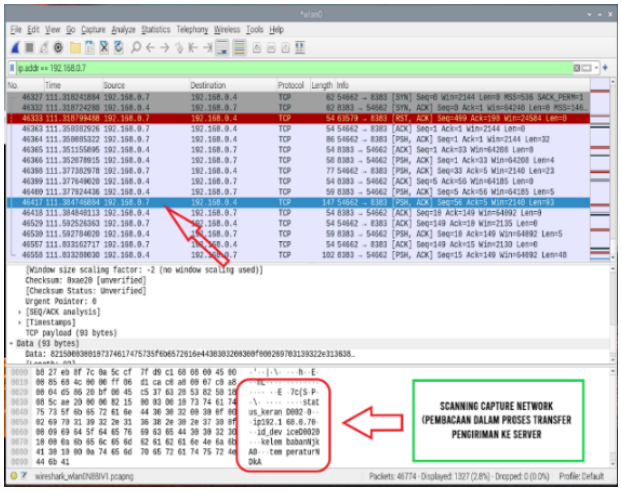
3.7 Skenario Pengujian Enkripsi Data Monitoring

Sebuah perusahaan saingan *Smart Farming* Budidaya jamur tiram A penasaran dengan perusahaan *Smart Farming* Budidaya jamur tiram B karena penjualan yang pesat dengan kualitas jamur tiram yang sangat baik maka perusahaan B tersebut ingin melakukan peretasan dan mencoba untuk melihat isi server di perusahaan *smart farming* budidaya jamur tiram B. Maka peretas mengekseskusi server perusahaan smart farming budidaya jamur tiram tersebut dengan Melakukan pembacaan data menggunakan *tools* kalilinux *wireshark* untuk melihat bagaimana suhu dan kelembapan sehingga jamur pada perusahaan tersebut berkualitas.



Gambar 14 Capture data enkripsi sensor A Traffic Wireshark

Pada Gambar 14 adalah pengujian deteksi aliran jaringan menggunakan *tools kali linux wireshark* dimana tools tersebut dapat mendeteksi dan melihat data yang sementara dalam proses transfer ke server. Maka dengan pengujian ini data yang dikirim dari *Ip Address 192.168.0.6* data yang berhasil di deteksi dalam bentuk enkripsi atau tidak dapat dibaca.

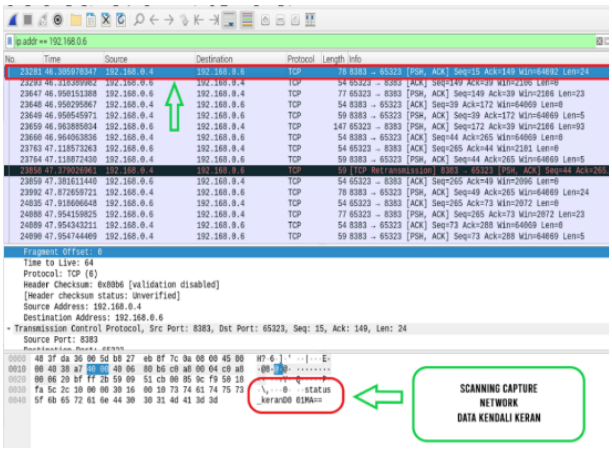


Gambar 15 Capture data enkripsi sensor B Traffic Wireshark

Pada Gambar 15 adalah pengujian deteksi aliran jaringan dari data sensor A dengan *Ip Address 192.168.0.7* menggunakan tools kali linux wireshark dimana tools tersebut dapat mendeteksi dan melihat data yang sementara dalam proses transfer ke server. Maka dengan pengujian ini data yang berhasil di deteksi dalam bentuk enkripsi atau tidak dapat dibaca.

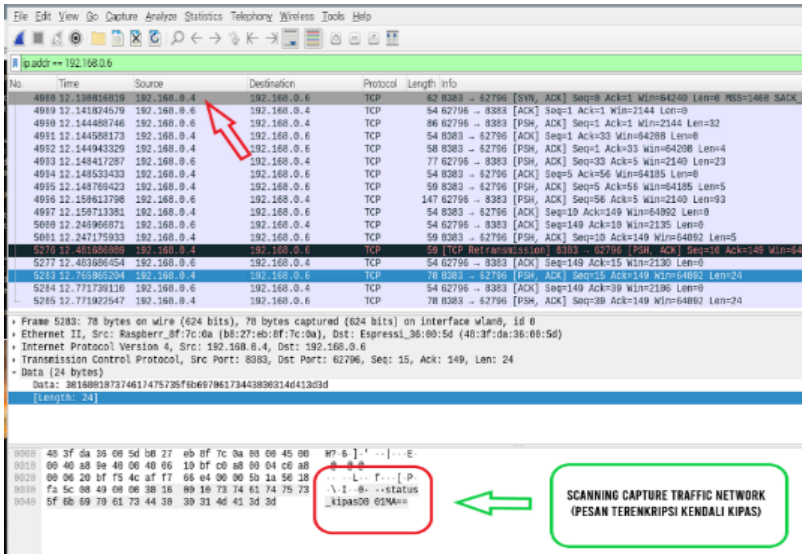
3.8 Skenario Pengujian Enkripsi Base64 Pesan Kendali

Sebuah perusahaan saingan *Smart Farming* Budidaya jamur tiram A penasaran dengan perusahaan *Smart Farming* Budidaya jamur tiram B karena penjualan yang pesat dengan kualitas jamur tiram yang sangat baik maka perusahaan B tersebut ingin melakukan peretasan dan mencoba untuk melihat isi server di perusahaan *smart farming* budidaya jamur tiram B. Maka peretas mengekseskusi server perusahaan smart farming budidaya jamur tiram tersebut dengan Melakukan pembacaan data untuk melihat bagaimana dan apa saja kendali yang dilakukan pada kumbung jamur tiram sehingga produknya berkualitas.



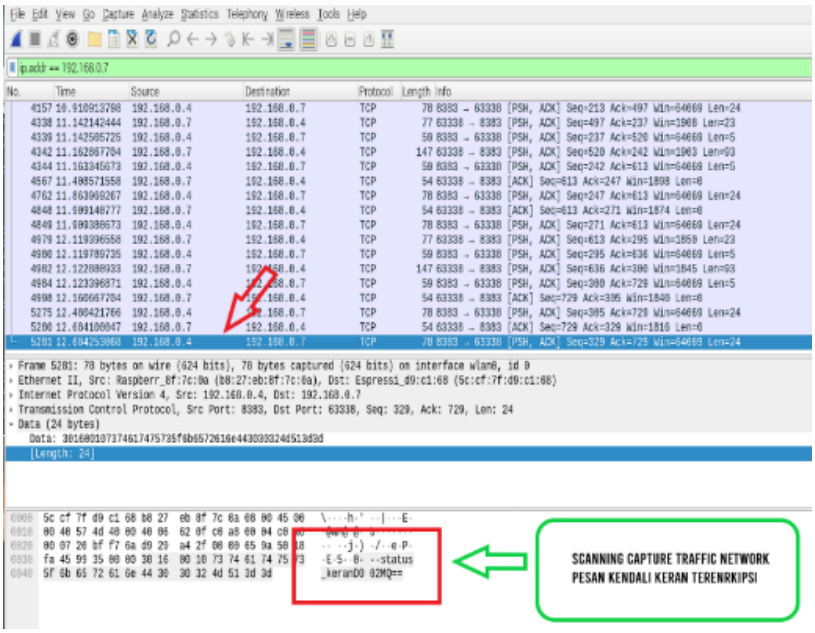
Gambar 16 Capture kendali keran terenkripsi Sensor A Traffic Wireshark

Pada Gambar 16 adalah pengujian deteksi aliran jaringan menggunakan tools kali linux wireshark dimana tools tersebut dapat mendeteksi dan melihat data yang sementara dalam proses transfer ke server. Maka dengan pengujian ini pesan kendali keran yang dikirim dari *Ip Address 192.168.0.7* data yang berhasil di deteksi dalam bentuk enkripsi. atau tidak dapat dibaca.



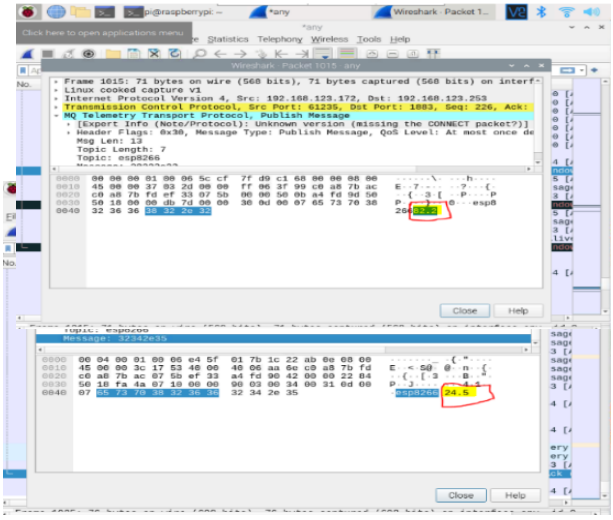
Gambar 17 Capture kendali kipas terenkripsi Sensor A Traffic Wireshark

Pada Gambar 17 merupakan pengujian deteksi aliran jaringan menggunakan tools kali linux wireshark dimana tools tersebut dapat mendeteksi dan melihat data yang sementara dalam proses transfer ke server. Maka dengan pengujian ini pesan kendali kipas yang dikirim dari *Ip Address 192.168.0.6* data yang berhasil di deteksi dalam bentuk enkripsi atau tidak dapat dibaca.



Gambar 18 Capture Kendali keran terenkripsi Sensor B Traffic Wireshark

Pada Gambar 18 adalah pengujian deteksi aliran jaringan menggunakan tools kali linux wireshark dimana tools tersebut dapat mendeteksi dan melihat data yang sementara dalam proses transfer ke server. Maka dengan pengujian pesan kendali keran yang dikirim dari sensor B dengan *Ip Address 192.168.0.7* data yang berhasil di deteksi dalam bentuk enkripsi atau tidak dapat dibaca.



Gambar 19 Capture tanpa enkripsi BASE64 sensor A Traffic Wireshark

Pada Gambar 19 merupakan pengujian tanpa enkripsi Base64 dengan menggunakan *capture traffic network* untuk melihat aliran jaringan Ketika Esp 8266 mengirim data ke server raspberry pi. Dapat dilihat bahwa data dalam proses transfer tanpa menggunakan enkripsi Base64 maka sangat mudah untuk melakukan pembacaan data menggunakan *wireshark.*

3.8 Hasil Pengujian Enkripsi Base64

1. Sensor A

Tabel 2 Hasil Pengujian data monitoring sensor A

No	ID_Device	Suhu	Kelembapan
1	D001	NzMA	NjYA
2	D001	NZuA	NTUA
3	D001	NzQA	NjmA
4	D001	NjCA	NTKA
5	D001	NzQA	NDYA

Pada Tabel 2 merupakan sebuah hasil pengujian data monitoring pada sensor 1 atau Esp 8266 Id device 001. Data yang dihasilkan merupakan data yang berhasil diamankan menggunakan Enkripsi Base64. Dapat lihat pada nomor 1 menunjukkan data suhu NzMA yang merupakan hasil enkripsi dari 26℃ dan data kelembapan menunjukkan NZuA yang merupakan hasil enkripsi dari 74%.

2. Sensor B

Tabel 3 Hasil Pengujian enkripsi data sensor 2

No	ID_Device	Suhu	Kelembapan
1	D002	NzuA	NTUA
2	D002	NTUA	NJAA
3	D002	NTMA	NJEA
4	D002	NDMA	NTGA
5	D002	NTUA	NTCA

Pada Tabel 3 merupakan sebuah hasil pengujian data monitoring pada sensor 2 atau Esp 8266 Id device 002. Data yang dihasilkan merupakan data yang berhasil diamankan menggunakan Enkripsi Base64. Dapat lihat pada nomor 1 di Tabel 4.4 menunjukkan data suhu NzuA yang merupakan hasil enkripsi dari 28°C dan data kelembapan menunjukkan NTUA yang merupakan hasil enkripsi dari 78%.

3. Hasil Enkripsi Pesan Kendali sensor A

Table 4 Hasil Pengujian enkripsi pesan kendali sensor

No	ID_Device	Keran	Kipas
1	D001	MQ==	MA==
2	D001	MA==	MA==
3	D001	MQ==	MA==
4	D001	MQ==	MA==
5	D001	MA==	MA==

Pada tabel diatas merupakan sebuah Hasil Pengujian enkripsi pesan kendali sensor 1 atau Esp 8266 Id device 001. Data yang dihasilkan merupakan data yang berhasil diamankan menggunakan Enkripsi Base64. Dapat 73 lihat pada nomor 1 di Tabel 4.5 menunjukkan data kendali keran MQ== yang merupakan hasil enkripsi dari 0 (Nonaktif) dan data kendali kipas menunjukkan MA== yang merupakan hasil enkripsi dari 1 (Aktif).

4. Hasil Enkripsi Pesan Kendali Sensor B

Table 5 Hasil Pengujian enkripsi pesan kendali sensor

No	ID_Device	Keran	Kipas
1	002	MA==	MQ==
2	002	MA==	MA==
3	002	MQ==	MQ==
4	002	MA==	MA==
5	002	MQ==	MA=

Pada tabel diatas merupakan sebuah hasil pengujian kendali pada sensor 2 atau Esp 8266 Id device 002. Data yang dihasilkan merupakan data yang berhasil diamankan menggunakan Enkripsi Base64. Dapat lihat pada nomor 1 di Tabel 4.6 menunjukkan data kendali keran MA== yang merupakan hasil enkripsi dari 1 (Aktif) dan data kendali kipas menunjukkan MQ== yang merupakan hasil enkripsi dari 0 (Nonaktif).

3.9 Pembahasan

Metode Enkripsi di impelementasikan dengan upaya menjaga data agar tidak ada seorang pun yang dapat membaca data Ketika dalam proses pengiriman. Mekanisme kerja yang dilakukan Enkripsi Base64 ini yaitu Ketika ESP 8266 telah menerima data dari sensor DHT 22 maka data yang awalnya dalam bentuk angka akan otomatis terconvert menjadi bentuk string dan huruf acak yang tidak dapat dibaca. Ketika data itu dikirim ke server raspberry pi dalam keadaan telah di enkripsi atau tidak bisa dibaca. Data tersebut telah sampai ke server MQTT dan database mysql akan terjadi sebuah pembuka atau kunci dari enkripsi yang disebut deskripsi, dengan tujuan agar Ketika *User Interfaces* melakukan pemanggilan untuk ditampilkan maka data yang dikirim dalam bentuk enkripsi tadi akan ter convert menjadi data deskripsi atau data yang bisa di baca. Pengujian enkripsi telah dilakukan menggunakan tools kali linux *Wireshark scanning* aliran data yang dikirim dan terlihat jelas data yang dikirim dari ESP 8266 terenkripsi atau data dalam bentuk acak yang tidak bisa dibaca. Jika dibandingkan dengan

sistem *Smart Farming* tanpa enkripsi Base 64 maka sangat mudah untuk dibaca menggunakan *tools kali linux wireshark* sehingga seseorang dapat melihat data asli dan kondisi keadaan kumbung jamur budidaya jamur tiram.

Berdasarkan hasil penelitian *Secure Wireless Sensor Network* pada budidaya jamur tiram yang telah di uji metode enkripsi Base64 dapat disimpulkan bahwa dapat mengamankan data dengan cara melakukan Enkripsi atau huruf acak yang tidak dapat dibaca Ketika dalam proses transfer dan server.

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Pada penelitian ini telah berhasil menerapkan Enkripsi Base64 pada sistem *Smart Farming* Budidaya jamur tiram dengan cara kerja data yang akan dikirim dari ESP 8266 akan ter enkripsi lalu dikirim ke server raspberry pi dan Ketika sampai pada server raspberry pi, database Mysql lalu *(User Interfaces) UI* melakukakan panggilan untuk ditampilkan pada halaman monitoring maka secara otomatis key enkripsi yang telah deprogram pada ServerMQTT akan bekerja sehingga data yang ditampilkan adalah data yang bisa dibaca atau dalam bentuk data asli.

4.2 Saran

Dari hasil beberapa implementasi keamanan yang dilakukan, adapun saran dari penulis adalah perlunya jaminan integritas data dengan menggunakan Digital Signature.

REFERENSI

[1] A. Lukman dan Y. Bachtiar, "Analisis Sistem Pengelolaan, Pemeliharaan dan Keamanan Jaringan Internet Pada IT Telkom Purwokerto," EVOLUSI, vol. 6, no. 2, 2018, doi: 10.31294/evolusi.v6i2.4427.

[2] Rosmiah, I. Aminah, Dasir, dan Hawalid, "Budidaya Jamur Tiram Putih (Pluoretus Ostreatus) Sebagai Upaya Perbaikan Gizi Dan Meningkatkan Pendapatan Keluarga," ALTIFANI, vol. 1, no. 1, Des 2020, doi: 10.32502/altifani.v1i1.3008.

[3] B. Bagaskara, Implementasi Wireless Sensor Network Untuk Budiday Jamur Tiram. yogyakarta, 2019.

[4] B. Chaniago, "Penggunaan Teknologi Wireless Sensor Network (WSN) dan GSM Pada Konsep Smart City," jumanji, vol. 2, no. 2, hlm. 135, Jan 2019, doi: 10.26874/jumanji.v2i2.40.

[5] Y. Wibowo, F. E. Prasetyadana, dan B. Suryadharma, "Implementasi Monitoring Suhu dan Kelembaban pada Budidaya Jamur Tiram dengan IOT," JTEP-L, vol. 10, no. 3, hlm. 380, Sep 2021, doi: 10.23960/jtep-l.v10i3.380-391.

[6] A. Wahid, E. Firdaus, dan J. Parenreng, "Implementation of Wireshark and IP tables Firewall Collaboration to Improve Traffic Security on Network Systems," 2021.

[7] A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," SST, vol. 4, no. 3, hlm. 110, Jun 2018, doi: 10.36722/sst.v4i3.280.

[8] A. Lutfi, E. Sakti, dan R. Siregar, "Analisis Mekanisme End-To-End Security Pada Komunikasi Antara Node Sensor Dengan IoT Middleware," 2018.

[9] Y. Rizaldi dan I. Febry, "Implementasi Multichain sebagai Alternatif Solusi Keamanan dan Privasi Data pada Komunikasi Perangkat Pintar Rumah," JINACS, vol. 1, no. 02, hlm. 115–121, Jan 2020, doi: 10.26740/jinacs.v1n02.p115-121.

[10] B. Nurcahyo dan S. Amini, "Implementasi Kriptografi Dengan Algoritma Base64 Dan Advance Encryption Standard Untuk Mengamankan Data Email Berbasis Web," vol. 1, no. 3, hlm. 8, 2018.

[11] R. Dhall dan V. K. Solanki, "An IoT Based Predictive Connected Car Maintenance Approach," IJIMAI, vol. 4, no. 3, hlm. 16, 2017, doi: 10.9781/ijimai.2017.433.

[12] A. Wahid, I. juliady, S. Gunawan, dan J. Parenreng, "Secure Wireless Sensor Network using Cryptography for Smart Farming Systems," IOTA, vol. 2, no. 4, hlm. 248–262, 2022, doi: 10.31763/iota.v2i4.554.

[13] M. Rakha, R. Munandi, dan A. Irawan, "Analisis Algoritma Advanced Encryption Standard (Aes) Untuk Sistem Pemantauan Konsumsi Daya Listrik Analysis Of Aes Algorithm For Electrical Power Consumption Monitoring System," 2020.
[14] A. Amzeri, "Pencegahan Serangan Denial Of Service Menggunakan Rule Based Signature Analysis Pada Jaringan Internet Of Things.," 2021.
[15] A. Wahid, Y. Sengoku, dan M. Mambo, "Toward Constructing a Secure Online Examination System," 2015.